DOCUMENT RESUME

ED 225 300 EA 015 371

TITLE	Report on the National Symposium on Personal Privacy and Information Technology (October 4-7, 1981).
INSTITUTION	American Bar Association, Washington, D.C.; American Federation of Information Processing Societies, Montvale, N.J.
SPONS AGENCY	National Endowment for the Humanities (NFAH), Washington, D.C.; National Science Foundation, Washington, D.C.
PUB DATE	82
GRANT	NSF-OSS-7924514
NOTE	24p.; For related document, see EA 015 292.
PUB TYPE	Collected Works - Conference Proceedings (021) -- Viewpoints (120)
EDRS PRICE	MF01/PC01 Plus Postage.
DESCRIPTORS	*Confidentiality; Data Collection; Ethics; Information Processing; *Information Services; Information Utilization; Laws; *Legal Problems; *Privacy; Social Values; Standards; *Technology

ABSTRACT

A national symposium was held October 4-7, 1981, to explore the relationships among law, ethics, and informational technology as they relate to the individual's informational privacy. The introduction to this report describes the conference format; discusses the Privacy Act of 1974 and the Freedom of Information Act; and offers definitions of personal information, privacy, confidentiality, security, access, and disclosure. Charles W. Joiner's opening remarks on "Personal Privacy and Information Technology," covering the purposes of the symposium, are presented next. The document then reports the conference's discussions on "Informational Privacy: Concepts, Values, and Technology," in which the conferees agreed that expectations and concepts about privacy differ. The document's recounting of the discussion of "Current Practices for Information Dissemination and Control" indicates agreement that informational privacy is relatively unprotected. Under "Considerations for Future Action," the report notes conferees' agreement that long-term mechanisms are needed to develop informational privacy policies, and outlines their discussion of privacy controls by government, personal self-help, or the private sector. Two appendices present a list of symposium participants and brief summaries of the conference's four background papers by George B. Trubow, Fred W. Weingarten, Alfred R. Louch, and Willis H. Ware. (RW)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

U.S. DEPARTMENT OF EDUCATION
NATIONAL INSTITUTE OF EDUCATION
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

This document has been reproduced as received from the person or organization originating it.
Minor changes have been made to improve reproduction quality.

- Points of view or opinions stated in this document do not necessarily represent official NIE position or policy.

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

Marna S. Tucker

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

Report on the National Symposium on Personal Privacy and Information Technology

October 4-7, 1981

Sponsored By

American Bar Association's
Section of Individual Rights and Responsibilities

Committee on Privacy

Elmer Oettinger, Jr., Chairman
Floyd Abrams
Martha Barnett
Barry Boyer
Charles Joiner
Mary Lawton

and

American Federation of Information Processing Societies

Special Committee on the Right to Privacy

Lance Hoffman, Chairman
Gordon Everest, Vice Chairman
Paul Armer
Robert Belair
Robert Bigelow
Robert Blanc
Robert Campbell
Robert Goldstein
Pender McCarter
William Moser
William Perry
Robert Smith
Rein Turn
Fred Weingarten

Support for the Symposium was provided by the National Science Foundation and the National Endowment for the Humanities, NSF Grant Number OSS-7924514. Any opinions, findings, conclusions or recommendations expressed herein are those of the authors and do not necessarily reflect the views of the National Science Foundation or the National Endowment for the Humanities.

This report has not been approved by the House of Delegates or the Board of Governors and, until approved, does not constitute the policy of the American Bar Association.

Copyright © 1982 American Bar Association

Library of Congress Catalog Card No. 82-74078
Section of Individual Rights and Responsibilities
Report on the National Symposium on
Personal Privacy and Information Technology
Washington, D.C.

TABLE OF CONTENTS

Preface i

Acknowledgments ii

Introduction 1

Opening Remarks:

Personal Privacy and Information Technology 2

Discussion:

Informational Privacy: Concepts, Values and Technology 5
Current Practices for Information Dissemination and Control 6
Considerations for Future Action 8

Appendix A: Roster of Participants 11

Appendix B: Summaries of Invited Papers:

The Development and Status of Informational Privacy Law and Policy in the United States 12
Information Technology and Privacy Trends in Products and Services 14
Morality and Privacy 15
A Taxonomy for Privacy 16

PREFACE

This report culminates yet another project initiated by the American Bar Association's Section of Individual Rights and Responsibilities (IR&R), this time executed with the support and cooperation of the American Federation of Information Processing Societies (AFIPS). IR&R has undertaken a variety of programs during the last several years related to threats to individual privacy posed by the awesome proliferation of personal information. AFIPS has for many years been concerned with privacy aspects of information processing as well, and the ABA/AFIPS partnership in this particular project is most gratifying.

The increasing concern about personal privacy during the last decade has stimulated much discussion and inquiry. Because ethics, science, and the law all must be involved in policy formulation to develop a concept of informational privacy in the computer era, a dialogue between those disciplines could help to explore the subject of "privacy" and perhaps lay some foundation for a better understanding of the concept. Thus, ABA and AFIPS organized an interdisciplinary dialogue which was conducted on October 4-7, 1981 at Amelia Island Plantation in Florida.

This project began with an idea developed by Daniel L. Skoler, then director of ABA's Division of Public Service Activities (of which IR&R is a part), Professor George B. Trubow, of the John Marshall Law School, an advisor to IR&R and the IR&R Privacy Committee, then under the chairmanship of Judge Charles W. Joiner. After exploratory inquiries received interest from the National Science Foundation's Program in Ethics and Values in Science and Technology and the National Endowment for the Humanities, a grant proposal was developed. AFIPS, through Dr. Lance J. Hoffman, professor of computer science at George Washington University and chairman of the AFIPS Privacy Committee, responded to the ABA's invitation to join in the effort. Dr. Elmer R. Oettinger, Jr., Professor Emeritus of Public Law and Government and former Assistant Director of the Institute of Government at the University of North Carolina at Chapel Hill, became chairman of the IR&R Privacy Committee while the grant was in process and carried the project forward. Together ABA and AFIPS personnel finished the planning and execution of the program. Professors Hoffman and Trubow co-directed the project, and Judge Joiner was chairman of the planning committee and privacy symposium.

At the opening of the symposium, background papers on law, ethics, and technology were presented by Professor Trubow, Professor Alfred R. Louch, Chairman of the Philosophy Department, Claremont Graduate School, and Dr. Fred W. Weingarten of Information Policy, Inc. These papers served to establish some cross-walks between the disciplines with respect to informational privacy. Dr. Willis H. Ware of the Rand Corporation then presented a paper that suggested a framework for examining informational privacy. The complete papers are not made part of this report, but are available separately through the ABA's Section of Individual Rights and Responsibilities as excellent resource documents in "Invited Papers on Privacy: Law, Ethics, and Technology." The purpose of this report is to focus on the results of the conference dialogue.

Professor Trubow served as conference reporter and prepared the draft report which was reviewed by a committee composed of Judge Joiner, Professors Hoffman and Louch and Dr. Weingarten. A revised report was circulated to all conferees for their comment, and the review committee gathered these comments to shape the final report.

The ABA's Section of IR&R and the AFIPS Privacy Committee are pleased to have cooperated in stimulating the examination of this very important subject. As society becomes more crowded and complex and information is more freely exchanged and disseminated, it seems certain that individual privacy will be subject to increased pressure and perhaps diminution. We believe that an increasingly open society desires an improved and advanced quality of life, yet needs to maintain an appropriate respect for individual privacy as a cherished human value. It is to that end that this project was sponsored, and we are most grateful to the National Science Foundation and the National Endowment for the Humanities for support of this worthy effort.

Dr. Elmer R. Oettinger, Jr.
Chairman, IR&R Privacy Committee

Dr. Lance J. Hoffman
Chairman, AFIPS Privacy Committee

ACKNOWLEDGMENTS

Soon after this project began, Daniel L. Skoler, who had been a prime mover as Director of ABA's Division of Public Service Activities, left that post. Ms. Katherine McG. Sullivan became Director, and she continued the excellent support and cooperation which the program had enjoyed. Janis I. Wise, staff associate of IR&R, provided excellent administrative assistance and liaison during the project and at the symposium itself. Without her help, this effort would have suffered markedly. My colleague, Lance J. Hoffman, did a stellar job as co-director of the project, and his efforts enriched the program and certainly made my life easier. As always, the wise counsel of my friend Elmer R. Oettinger, Jr., the IR&R Privacy Committee chairman, helped us steer a good course. Judge Charles W. Joiner, conference chairman, whose good humor and expert leadership kept the conference in pursuit of planned goals, deserves special accolades. Without the help of discussion group leaders and reporters Judge George N. Leighton, Robert Belair, Martha W. Barnett, Donn B. Parker and M. Granger Morgan, the substance of the conference could not have been captured and organized. Diane Gordon, faculty secretary supervisor at John Marshall Law School, provided her amiable and dependable help, and Peggy Schmitz, faculty secretary, typed the report drafts. To all these people I express my sincere appreciation and thanks.

In conferences where the divergent opinions of established experts are expressed on complex topics, it is not unusual for discussions to become loud and lively. This symposium was no exception. To all the conference participants I pay sincere homage for their cooperative spirit and unflagging attention that made this not only a worthwhile intellectual effort, but a pleasant and congenial professional endeavor.

George B. Trubow
Reporter and Co-director

INTRODUCTION

Almost everyone seems to be talking about privacy today, but the word is used in a variety of ways. Wiretapping, the right to an abortion, and the confidentiality of financial information have all been referred to in a "privacy" context. Thus, privacy might refer to the exclusiveness of "space" around an individual, the autonomy of decision making without government interference, or the expectation that certain personal information will not be shown to outsiders. It is in the latter sense that the ABA/AFIPS symposium considered the question of privacy. To a large extent an individual is known to others as a composite of the information that describes him. Especially in the modern "information society" where computers make information easy to store, manipulate, use, and distribute, individuals are increasingly worried about who has information concerning them, how it was obtained, and to what uses it will be put.

There is no accepted intellectual foundation for the notion of informational privacy. It is this reality that led the ABA, with AFIPS endorsement, to apply to the National Science Foundation for a grant to conduct an interdisciplinary symposium to explore informational privacy. Because the concept of informational privacy is defined by the confluence of ethics, social science, technology, and law, representatives from those disciplines gathered for three days to explore the concept and suggest ways in which it could be more clearly defined and in which the interests of society and the individual could be better protected.

Three background papers were presented: Professor George B. Trubow delivered a paper on the legal aspects of informational privacy in the United States; Dr. Fred W. Weingarten considered current and future communications and computer technology; and Professor Alfred R. Louch discussed moral and ethical concepts relevant to the notion of informational privacy. The complete papers are not reprinted here since this report focuses on the symposium discussions. The background papers were published separately by the ABA's Section of Individual Rights and Responsibilities and are available in "Invited Papers on Privacy: Law, Ethics, and Technology." To give a flavor of their content, however, brief synopses of the papers are presented in Appendix B of this report.

Following the initial background session, wherein the foregoing papers were discussed, the participants were divided into three discussion groups, each of which included representation from the disciplines present at the symposium. After a day of group discussions, the participants met again in plenary session to compare notes, report on progress, and reevaluate symposium objectives. At that time, Dr. Willis H. Ware, a scientist with The Rand Corporation and previously vice-chairman of the Privacy Protection Study Commission, presented a paper which suggested how law, technology, and ethics might be harmonized in a framework for informational privacy. Dr. Ware's remarks were intended to provide added stimulus to the continuing symposium dialogue. A condensation of his paper also appears in Appendix B.

Subsequent to discussion of the Ware construct, there was a second day of small group discussions. The participants met in a final plenary session to hear from each of the groups and to consider findings and recommendations. The discussion was organized to focus on the meaning and significance of informational privacy, the current practices regarding the control and dissemination of information, and considerations for future action with respect to the development and protection of informational privacy.

This report is based upon the transcript of the final session of the symposium.

Before moving to the body of the report, it will be useful to clarify some terms as used in this document. The phrase "personal information" means any information that can be referenced to an identifiable individual by use of name, number or other characteristic. That which makes information personal is not its content, but whether it refers to a specific identifiable person. The word "privacy" relates to people and considers what and how personal information is gathered and how it is used. One's privacy may be violated if, for example, improper or inaccurate information is collected. The word "confidentiality" refers to the sensitivity status of information and the circumstances wherein one other than the data subject or record holder inspects or uses personal information. The word "security" is often linked with privacy and relates to the protection of information in a record keeping system. Security prevents unauthorized disclosure, alteration or loss of data and, thus, security attempts to assure confidentiality and integrity of data.

When one can inspect or use information, one has "access" to it. Information is "disclosed" by a record holder to one who seeks access to it. Dissemination and disclosure are similar but the former implies a wider distribution of information, at times on the initiative of the record holder.

This report often refers to the Privacy Act of 1974 and to the Freedom of Information Act. The former covers personal information in certain record systems maintained by or for the federal government. The purpose of that Act is to assure that principles of privacy, confidentiality, and security, to be discussed below, are observed by federal agencies in connection with the collection, storage, use, and disclosure of personal information. In brief, the Act allows a data subject to have access to files about himself, requires a procedure whereby incorrect or obsolete data can be amended or discarded, and restricts the use and dissemination of personal information maintained by federal agencies.

The Freedom of Information Act (FOIA), first enacted in 1966, is basically a disclosure statute. It presumes that information held by a federal agency should be available to the public, with specific exceptions to disclosure for protection of interests such as national security, trade secrets, and proprietary infor-

mation, or personal privacy. In effect, the FOIA says that the government's business is everyone's business. The Privacy Act, on the other hand, presumes that personal information is nobody else's business and should be disclosed only pursuant to the data subject's consent or specific provisions of law.

We now turn to the symposium itself. We begin the summary of discussions at Amelia Island with the opening remarks to the participants made by the conference chairman, Judge Charles W. Joiner.

Opening Remarks

Personal Privacy and Information Technology

by Charles W. Joiner

Initially, let me suggest what this conference is not. It is not a conference to deal with the horribles about privacy invasions by the press or computers. It is not a conference to explore ways and means that computers can be made better—either in the sense of holding more information or retrieving it more rapidly.

I think it is not a conference primarily to study the ways and means of record keeping to make information storage and retrieval more safe, nor even to hear how computers can be made more secure, nor to plan to serve society better through the use of the computer.

This is a conference about people, about individuals, about human beings, about men and women who have developed a gloss imprinted on their souls called *culture* and who live together in a *civilization*, each of whom has in some manner achieved a bag of *values* they carry with them until some of them may be lost.

We are here, I believe, to be talking about you and me and each of the rest of us as individuals, about our values and our culture and our civilization, and about how this new science of information technology is affecting us individually—how it's affecting the values that we hold, how this affects our culture and our civilization, and how it can be used to the benefit of individuals rather than to destroy their souls.

I feel quite out of place talking to you about these matters. Each of you is here because of some special expertise, some of you as "the authority" in the field of privacy itself. At the risk of offending the rest of you, I humbly acknowledge that any contribution I can make pales before the contribution of my friends, Alan Westin and David Linowes. So, I go forward as one voice carrying with it all the baggage of the values I have developed as a result of my experiences, learning, and the culture to which I have been exposed.

The dialogue we are to have is on personal privacy and information technology. We are here because the Section of Individual Rights and Responsibilities of the American Bar Association requested the National Science Foundation's Program in Ethics and Values in Science and Technology to finance this program. In requesting funds, we have made the following representations:

1. There is a feeling that the basic social values are being threatened by data storage, retrieval, and communications technology.
2. There is a worry that developments in data technology threaten social values of privacy, autonomy, and our conviction about the right to be left alone.
3. There is a fear that the rapid development of technology will outstrip our capacity to foresee and prevent unintended abuses, citing Linowes, Orwell, and public opinion polls.

The application then proceeded to list a number of questions about efforts to deal with this problem. We asserted that there was a reason to question whether the legal profession (the legislators, the practitioners, and the courts), acting largely alone, can deal with the complexities and refinements of the problem.

We suggested that it was not clear that the laws and regulations and judicially-created remedies are an effective solution. It may be desirable to foster the development of ethical codes and precepts for the various data handling professions which may in turn affect the efficiency of the data storage and retrieval system itself.

We represented that there was reason to believe that there was insufficient discussion among persons in the fields of ethics, morals, philosophy, anthropology and the "doers" (those creating the hardware and software) and "controllers" (the legislatures and the courts) to respond to the problems.

We indicated that there is a feeling that efforts have too often focused on the dilemma of society's need to know and society's need for privacy and not enough on the dilemma of the "individual human being's need to be private" as against the individual's need that society should know.

We suggested that the Section of Individual Rights and Responsibilities would convene a group of persons to provide intellectual interaction and dialogue:

1. to understand and define the basic issues at stake, and
2. to explore the relative merits of legal and non-legal approaches to these problems.

So we are here today with the additional help from the American Federation of Information Processing Societies to focus on that problem—the individual's privacy needs and values on the one hand, as against the individual's need for society to have information to provide for other individual needs and values on the other hand. The individual is on both sides of the dilemma.

It seems to me that central to what we are talking about at this meeting is the individual, not the corporation or the government. The hardware and software of the system that stores, retrieves, and communicates information is not central. The beginning point, the central point, is the individual. We are interested in the autonomy of the individual but not in the sense that his privacy actions are impinged upon by legislative proscription against contraception information or abortion, or against his right to read, or against his right to be free to act by choice in his home. We are interested in the narrow but important problem of the effect on that individual of information technology and the effect that data storage and retrieval (the technology of communication) has on him or her as an autonomous person, and whether that effect is good or bad, and how we can best respond as a society to this problem.

We are interested in this in two respects, one of which contains several parts:

First, we are interested in understanding what have been and are the individual values relating to privacy.

Second, we are interested in determining how, if at all, current and projected use of data storage, retrieval, and communication systems will affect that individual and his or her values.

1. We want to know if that person has changed, or will change as a person as a result of data storage and retrieval ability of the computer and the new communication systems and, if so, how, and—if we can determine—is this change good or bad.

2. We want to know if and how that person's expectations of society are enhanced or depressed by the data and communication systems and what expectations for the future we might have from such change.

3. We are interested in the conflict, if any, between these two and how that conflict can be ordered and controlled.

But above all, I think we are here always to keep in the forefront the individual, the person, that person as a private individual, but also that person as a gregarious individual who forms tribes, groups, and governments, develops cultures and civilizations, and seems to have a need to relate closely with others, to give others information so that others can make safe and enrich the life of the individual.

When I was younger and had more energy, my wife and I would on occasion devote some time to organized study of selected topics. I remember a wonderful experience in the mid-1950's in which we attempted to learn something about the humaneness of the human being. We became a part of a group sponsored by the Fund for Adult Education, reading selected materials and discussing the problem. We studied an excellent collection of essays, textbooks and research papers entitled "The Way of Mankind." The writers of these papers were all distinguished anthropologists, philosophers, or sociologists. It was exciting, but in attempting to help us understand the ways of mankind there was no mention of privacy, absolutely none; even in the chapters dealing with culture, technology, values, ethics, and society, there was nothing on privacy. This was true even though George Orwell and Aldous Huxley had raised the ugly head of the subject for the public to see. In the mid-1950's learning about the ways of mankind, privacy was not worth talking about.

Today all that has changed. Largely but not entirely because of the computer, we have been reassessing the place of privacy in our system of values and are redetermining when and how it fits into the ethical considerations of our society.

Each of us develops a value system from those who are around us and from the events we observe, and we learn about that which seems relevant to us. Society takes the value systems of the group, excluding a few non-conformists, and ethical considerations arise from which we ultimately adopt laws and regulations to govern our lives. It is clear to me that the value system as it relates to privacy has undergone remarkable change in the last 20 years.

I hope that we can focus on the changing of the individual caused by the information gathering, retrieval, and communication systems. I hope that we can look at the individual values, not only to be a private person but also to be a part of a social group—aside from the individual's needs to relate to others so as to provide him food and clothing, medical attention, and other amenities of life. There is a deep felt need, I believe, for the individual to expose himself or herself to others and to be the recipient of confidences. A sense of caring and sharing is an important value.

It seems to me that we are here to discuss a subtle but important problem: Does the pervasive gathering of personal information about a person or the wide dissemination of that information adversely affect him or her as a person? Are we as individuals changing? Are we becoming more cynical, more open, more understanding, more sympathetic, more callous, more rebellious, more submissive? Is our ability to collect and process information and communicate it more widely a factor in our becoming more litigious? Can it have an affect on society's mores about marriage and living arrangements, about the birth rate, and others? These questions are without end; but as to each question answered "yes," another must be answered. Has the information gathering helped society to provide the things we want and need and treasure—for example, better health, less crime, more ease of travel? How should we balance the two answers and how can we control the balance?

Let us think about an individual in society today. At birth his name and date of birth, names of his parents, their address, are recorded. This is public. Every time he goes to the hospital or to the doctor for

treatment, a full record is made of everything done to him. Every time he flies, the date and place are recorded. When he attends school or college, detailed information is acquired and retained about him. If he ever has any contact with law enforcement officials, another detailed set of information is kept on him. When he learns to drive, he obtains a license, he gives his name, his address, and his date of birth, and usually a picture. This is kept up to date and is public. When he marries, his name, the spouse's name, their address, the fact of their passing a blood test, are all recorded along with the date. This, too, is public. When he first works, the government gets information that permits him to establish his Social Security file. If he works for the government, he may have a job that requires an FBI investigation and much more information is kept in his file. The Internal Revenue Service keeps all of his financial information. Every time he obtains a credit card or a bank loan or applies for insurance, detailed credit and personal information about him is gathered.

There are many more places where information is gathered and kept, but this recitation will be sufficient. All during his life, pictures and stories of anything he could do might be sent nightly into every living room in the country.

My question to you then is this: Has this person changed as a result of any or all of these advances in the technology of data processing and communication? Is he different than he would have been if this information had not been gathered? Would he be different if the information was all cross-interrelated and made more accessible? Is he different as an individual or in his ability to relate to others? Are his values changed? Are his expectations altered? And what about the future? Will he change a the predicted advances and uses of two-way computer controlled television communications become a reality? Has he benefited as a result of the advances in information retrieval and communications? How does it balance? How can it be controlled? Laws? Ethical standards? Proscription? Better hardware? Software? Regulations? Religious revival?

You have three fine advance papers. We will talk for three days. I hope we can contribute to the solution of the problem.

Discussion

Informational Privacy: Concepts, Values, and Technology

Privacy is a word of many meanings; people speak of physical privacy, emotional privacy, psychological privacy, and other types of privacy. In this report, the focus is on privacy dimensions whose existence arises from the collection, dissemination, and use of information—in particular, information about people.

Even if restricted to this information context, privacy is not a single concept or value. Privacy interests range on a continuum from the effect on one individual resulting from a decision about him based on personal information, to the general vulnerability of society resulting from the rapid development of information technology unconstrained by privacy considerations. Personal information kept in individually referenced files for the purpose of making decisions about the data subject obviously has a direct impact on the individual. For example, information in an employee's personnel file can be used to determine whether that person should be hired or fired, promoted, or retired. At the other end of the continuum, society may be vulnerable to the vast quantities of information made available by modern technology. The collection and use of marketing information may dictate the kinds of goods and services made available to or withdrawn from various segments of the population; the behavior or welfare of society can be affected by the use of information concerning buying habits or voting patterns.

Somewhere along this continuum, individuals may feel vulnerable to the collection of information not used immediately for any specific decision making process, but which might be used at some time in the future for a decision affecting such an individual. A participant expressed it this way:

> This category of concerns springs from the proliferation of computer and communication technologies that handle information about people and which can, through their very existence, subtly modify the way people behave. Some of us talked in terms of a chilling effect; I may be less outspoken or more circumspect in my public utterance and behavior if I believe that a large fraction of things that I do and say is being squirreled away in a variety of information systems. The value issues addressed here involve not so much direct threats to specific civil liberties but a subtle erosion of our ability to fully enjoy the full range of those liberties.

Retroactive guilt by association is one example of this category. The fact that A associates with B, recorded today in a file, may be of little concern. But perhaps a decade later, when B is then considered a social or political outcast, recall of the past association may then cause harm to A. The mere fact that personal information is stored in files involves the possibility that the information can be marshalled into a profile describing an individual. Who knows to what uses, by government or by the private sector, this profile might be put? During the symposium it was expressed this way:

> The mere existence of an automated data base containing personal information is in itself a privacy problem. An analogy can be made to nuclear material, which is a potentially hazardous material. By analogy, a threat exists with regard to the mere computerization of personal information because it stays there. What happens to it, the individual data subject doesn't know.

Although the differences between immediate impact on the individual, future vulnerability of the individual and the potential vulnerability of society at large can be appreciated, it is not always possible to separate various kinds of personal information into one or another of these categories. This adds to the complexity of understanding the problem and shaping a policy for informational privacy.

It was also observed that privacy values vary with time, place, and culture. Just as language changes over time and words unacceptable for public utterance a generation ago may be permissible today, so do the passage of time and the changing values of a people also change the expectations of privacy and the effects of data collection. One participant observed:

> The concept of privacy changes over time, and because of other factors. Privacy concepts are different geographically. The concept of personal privacy in one part of this country may be different than in another. It changes demographically. For example, people in a village or small town could have a very different concept than a person in a large city where one has more anonymity than in a small town.

Accordingly, informational policy must admit of sufficient flexibility to reflect the changing expectations and cultural values of people. Indeed, our institutions have disagreed about perceptions of privacy. One example involves the confidentiality of bank records: when the Supreme Court of the United States considered the issue, it held that a customer does *not* have a reasonable expectation that his bank record will be treated as private or confidential because it is but an aggregate of separate "public" transactions whereby the customer sends personal checks into the stream of commerce. On the other hand, on virtually the same question, the California Supreme Court held that a bank customer does expect confidentiality with respect to such records. The Congress of the United States agreed with the California Court, and in 1978 passed the Financial Privacy Act which in effect overturns the U.S. Supreme Court decision and gives a bank customer the expectation of confidentiality with respect to his bank records, though only in connection with inquiries by *federal* authorities.

Further, as discussed in the legal summary paper found in Appendix B, even though fair information practices have been articulated, they were developed to apply to government agencies and certain regulated businesses and not to the conduct of individuals in their private capacity. Now that the "personal computer" is growing in popularity today, and as more and more people purchase them for private use, a confrontation develops between two differing privacy interests: The person who operates a computer in his living room perceives that it is nobody's business what information he has and what he does with it. On the other hand, anyone about whom personal information is stored in a microprocessor in a neighbor's home may indeed have great concern about the potential for personal privacy violation.

If society becomes more "open," informational privacy may be of less concern. One discussion group said:

> Our group suggested that there is an evolution taking place in the social context which defines what privacy is, and that evolution is probably moving towards a more open society. While we disagreed about the extent to which a more open society would reduce the problems of privacy, we did agree that evolution alone is at least in the short run probably not sufficient to solve the problem . . . there probably will remain areas or pockets of privacy sensitivity for quite some time in the future.

American society today, however, is unprepared to declare itself "open" and considers that significant amounts of personal information are "nobody else's business." And even when information is "public" in the sense that anyone may observe it, an individual becomes concerned when this "public" information is aggregated and stored in a dossier. Who would be happy to learn that a complete list is being kept of the realty one owns, the clubs to which one belongs, the restaurants where one has eaten or the people with whom one has been seen, even though each of these separate items may be observed by the "public." Much depends upon who is keeping the records, why, and how they are being used.

Accordingly, the conferees agree that:

INDIVIDUALS HAVE VARYING EXPECTATIONS OF INFORMATIONAL PRIVACY: SOCIETY LACKS A CLEAR AND SETTLED USE OF THE CONCEPT.

Current Practices for Information Dissemination and Control

Given the uncertainty and ambivalence in defining privacy as a specific value, it is not surprising that information practices with respect to the confidentiality of personal information vary and are often conflicting.

For instance, each individual wants to make the determination as to whether personal information is relevant to a particular decision and should be supplied. That perception varies depending upon whether one asks or answers a question. When a prospective employer, for instance, asks questions of an applicant for a job, he expects full and complete answers to all questions. On the other hand, the prospective employee filling out a job application may desire to provide as little personal information as possible and to answer only those questions which he believes reflect favorably upon his chances for employment. The self interests of individuals may entail differing answers regarding what is or ought to be confidential. As a result, one would expect to find a wide variety of information practices.

The general public, as well as governmental authorities, appear to be hungry for information and want to collect great quantities of it without a full awareness as to what may be the results of such practices. Information in federal data banks often has been collected as the result of some general authorization by Congress in connection with a program of government regulation or service. In the private sector, prior to the Fair Credit Reporting Act (FCRA), many abuses arose from the conduct of certain credit reporting agencies that gathered and stored haphazardly and unreliably personal information which all too often surfaced in harmful and degrading ways. Although the FCRA prevents many abuses, most personal information maintained in the private sector is not subject to any regulation. The confidentiality of most banking information has limited protection only against federal inquiries. There are no federal regulations of health, employment, insurance, or general business records, and there is little state legislation providing practical protection in those areas.

Although the Carter administration proposed a series of bills designed to protect individual privacy in the public sector, none were enacted because grounds for consensus could not be found. For a decade Congress considered legislation to regulate the confidentiality of criminal justice information, but again no agreement could be reached for a balance between access and privacy. Regardless of the kind of personal information involved, there is someone who wants access to it and someone else who wants to shield it;

the conditions and exceptions regarding the supply and demand of information are subject to vagaries that complicate systematic regulation.

There are amazing incongruities in the application of principles of fair information practices. The Privacy Act of 1974 undertakes to implement the principles but applies them only to executive agencies and does not bind federal courts or the Congress. The same pattern of exempting the judiciary and the legislature from privacy legislation is typically found in those few states that have some sort of informational privacy laws. For instance, suppose an individual petitions a state court to have certain information expunged or purged from a state agency record. When the right is established, the court enters an order requiring the agency to expunge or purge so that the information is no longer available to the public. The order of the court, however, which specifically identifies the purged information, may be considered by the courts to be a public record and, as such, may be subject to public access. Although an individual's privacy right may have been recognized concerning information held by a state executive agency, that very same interest may be violated by the judiciary itself.

Likewise, although the political files that a congressperson or state legislator keeps probably contain a great deal of sensitive information about constituents, they are not subject to the constraints placed upon executive agency files. The pursuit of self interest (political, commercial and social) tends to make fair information practices uneven.

Conflicts in practice also result from the countervailing thrusts of privacy legislation and of freedom of information acts, whether at the federal or state level. Information in a government record may be presumed to be public, but personal information in the government record is likely to be considered confidential. Those differing presumptions may be justifiable, but they also are difficult to implement when an agency employee tries to decide whether a citizen's "right to know" supercedes another citizen's "right to privacy." One participant observed:

> One of the things that all of us have to realize in terms of practice is that privacy often depends upon the clerk in the records office, whether it's federal, state or local. In your register of deeds office or in some other office which holds records, that clerk operates under the law, state or federal, as he or she understands it. What goes on in the mind of that individual as to whether you get the record or not, or under what circumstances?

As previously noted, fair information practices have been agreed upon only to the extent to which they apply to government or certain regulated businesses. Accordingly, the individual who has a microcomputer at home does not consider himself subject to the same constraints as applied to government or business. The privacy right of the individual who stores in his personal computer information about others is in conflict with the privacy of those about whom he has the information. The conflict has yet to be balanced and resolved.

Even when an individual can rely on informational privacy rights as against organizations, his path is not easy. As one discussion group reported:

> A person today is at a disadvantage in an adversary relationship to organizations with great amounts of resources. It's often difficult for a person to show what his injuries really are if he is dealing with intangible privacy injuries; they don't leave bruises that can be visibly seen. And the process for challenging a wrong is lengthy and costly and the individual's position is further eroded.

While this uncertainty in policy and practice persists, information technology develops in awesome dimensions without practical constraints on behalf of informational privacy. Tiny microprocessors and integrated circuits residing in an apparatus smaller than a breadbox currently have more power and can outperform computers which a decade ago might have filled an entire floor in a large office building. Miniaturization and new techniques in electronic information storage devices permit vast quantities of information to be stored and processed at a speed so mind-boggling as to defy description. Satellites permit information generated in New York to be instantly available in California so that, in differing time zones, an event can be recorded "before" it happens. Although technology did not create privacy problems, it surely has escalated them dramatically, and that technology is being developed and used without adequate dedication to the control of privacy threats. Listen to this discussion among participants:

> PARTICIPANT NO. 1: Computer technology has brought a problem that we've always had into high visibility because of the cost effectiveness with which it can collect and process personal information and the cost effectiveness with which it can deal with information in very large amounts.
>
> PARTICIPANT NO. 2: The technology potential is there to control access and to control privacy. The computers provide that potential. But managers, holders of information, and controllers of information systems have to make decisions to allocate resources, to spend the time and money to implement those technical safeguards. When I look at current practice, the kinds of technical safeguards that are instituted in data processing systems, I find them to be quite inadequate, a long way from what might be possible. Certainly there are exceptions in some organizations . . . but I see many cases where they're not building safeguards.
>
> PARTICIPANT NO. 3: It seems to me that one of the most important problems with current practices has been illustrated by this discussion. As was pointed out, we're developing major information communication systems and writing policy for those systems, and privacy is not being considered. If people think that we can come along in 1990 and impose on top of those structures once they're go-

ing some omnibus privacy act to fix everything we discovered was wrong, they're naive. We need to be putting privacy considerations into all these decisions that we're making now about the nature of the information society we're building.

PARTICIPANT NO. 4: If I heard him correctly, he's saying that in the consideration of technological development, consideration should be given to privacy aspects at the time the system is developed.

PARTICIPANT NO. 5: I think it's got to be said much stronger than that. It's got to be said that privacy concerns must be an explicit design goal in all new information systems.

PARTICIPANT NO. 6: [Participant No. 3's] comments really concern me because what he describes is actually happening today. Congress is considering a communications act which will affect how communications are established in the next hundred years . . . Is what we're doing here going to be translated into something that has some impact? Is there time? I don't know.

PARTICIPANT NO. 4: I don't know either.

PARTICIPANT NO. 5: Decisions are being made right now.

PARTICIPANT NO. 4: We can't all get on an airplane and go to Washington today.

PARTICIPANT NO. 7: We need to step back and make sure that we don't go too far. The point is, regarding time to solve it, that as we sit here, information systems are being designed that will have an impact on privacy. These systems have to be under continual examination and there has to be a mechanism for making privacy protection explicit.

Further, there appear to be few limits on the future capacity or speed with which information technology develops. The conferees were, as a result, uncertain as to whether privacy had already been sacrificed for scientific achievement; they wondered whether the integrity of the individual had been exchanged for the "advancement of society." Although the conferees were not willing to concede that all was lost, nevertheless they did agree that:

"THE INDIVIDUAL'S INFORMATIONAL PRIVACY IS RELATIVELY UNPROTECTED AND WILL REMAIN SO UNLESS AN EFFECTIVE CONSTITUENCY IS DEVELOPED."

Considerations for Future Action

Throughout the discussions that took place during the symposium, the conferees repeatedly encountered clashes of interest that require fair balancing, problems that need further study and dialogue, and ideas in want of more examination and development. Consider the following excerpts:

PARTICIPANT NO. 1: I think there's a difference between there being an identifiable and active constituency and there being an enormous amount of public concern about people's lives being affected. One of the difficulties in mobilizing political action on the privacy issue is that constituencies are often people in groups that have a difficult time acting in their own behalf or even being able to put together the pieces of the puzzle of what's happening in their lives.

PARTICIPANT NO. 2: The public doesn't scream until it's hurt. Somebody had better get worried about it; the framework of values needs to be defined in greater detail, and it cannot be done in a two- or three-day meeting. Whatever we do here is at best a preliminary attempt to serve as a catalyst or as a town crier with an alarm bell to lead to a specific mechanism or mechanisms which can develop something much more tangible and effective.

PARTICIPANT NO. 3: There needs to be a mechanism through which there is public input or some kind of input into the development of systems which will contain personal information.

PARTICIPANT NO. 4: I think it has been said by everyone so far that people become concerned when they suffer some real harm, but there is no general public awareness of the vulnerability that arises simply because of the existence of data banks and the material that's in them. The suggestion was made earlier that it may require a kind of Three Mile Island disaster to bring this to the public awareness.

PARTICIPANT NO. 2: One-shot conferences have value. But they don't provide a continuum for new directions and actions. We need a practical mechanism or mechanisms whereby we can attempt to get at privacy problems that are the result of the technological revolution and perhaps of other things. We have to bring together interested groups and the public so that they're made aware of the problems.

PARTICIPANT NO. 5: A word that keeps popping up throughout the discussion is the word "mechanism," a mechanism for a continuing

analysis, a mechanism to balance the interests, a mechanism to do this or that. We seem to be searching for some sort of entity to assure that all these privacy problems are going to be looked after. On the one hand, we certainly don't want an information czar or a federal big brother. But yet, there is repeated recognition that we need something in terms of a formal institution.

Two notable efforts in the past, the HEW advisory committee's report in 1973 and the Privacy Protection Study Commission's report in 1977, were the results of sustained projects designed to examine informational privacy and to develop appropriate regulations. Nevertheless, those projects ended after several years, and their recommendations for improvement have been filed on bookshelves. Lacking a coordinated and continuing effort for implementation, little positive action has transpired during the last five years. The private sector has made some effort to improve its information practices, but nevertheless the finding previously stated appears to stand without significant challenge: the individual's informational privacy is relatively unprotected. What emerges as a significant consensus is this single but urgent recommendation:

SOME LONG-TERM MECHANISMS OR INSTITUTIONS, PUBLIC, PRIVATE, OR BOTH, MUST BE ESTABLISHED TO EXAMINE AND DEVELOP INFORMATIONAL PRIVACY POLICY THAT BALANCES GOVERNMENTAL, SOCIETAL AND PRIVATE INTERESTS.

□ □ □

Given the vague and general nature of privacy values and problems and the limited time for discussion, the symposium participants were unable to develop specific suggestions for particular mechanisms or institutions of continuity. The options for informational privacy protection include regulation by federal or state government, self regulation by the private sector, and self-help actions by individuals in pursuit of their own privacy interests. It is doubtful that an effective and balanced series of information controls will develop accidentally or as a result of pressures in the market place. A variety of informational privacy issues grow out of differing information usages and this seems to discourage the coalescense of an articulate constituency clustered around any particular subject matter. Here are some considerations that will affect the dynamics by which any institutions or mechanisms will be generated.

Controls by Government?

The conferees were hesitant to suggest the establishment of a federal agency whose responsibility would be to develop and monitor information policy. Congress has refused to establish any central agency with broad power to administer the Privacy Act; most people seem to shrink from the notion of a "federal information czar." The question of "who watches the watchers" is an important one.

With respect to governmental intervention, a threshhold question is whether federal or state regulation is desirable? When information crosses state boundaries it could be an incredible burden on citizens and the business community if varying protocols for the use of personal information had to be observed in different jurisdictions. The National Conference of Commissioners on Uniform State Laws perceived a need for uniformity in information regulation and recently proposed a uniform information practices code that undertakes to make consistent the notions of freedom of information and informational privacy. The proposed uniform code has an optional provision for the establishment of a state information practices commission. The drafters of the proposal appear to recognize the utility of such an agency, but made such a provision optional in recognition of the divided viewpoints regarding the wisdom of establishing such an agency.

Self-Help?

Apart from creating a federal agency to oversee informational privacy, Congress could simply extend the Privacy Act to the private sector, leaving it to individual citizens to protect their own privacy interests by elective enforcement of the law. As was pointed out earlier, the conferees recognized that private enforcement may place severe burdens on the individual however and may be a significant barrier to the protection of personal rights because of the time and complexity of litigation under the Privacy Act.

On the other hand, specific legislation might be enacted to deal with particular informational areas in the private sector such as health, insurance, employment, or criminal justice. Legislation on those subjects is once again pending in Congress, including a proposal to establish a federal agency to oversee the development and monitoring of information policy, but those proposals do not appear to have high priority because the Reagan administration does not favor new government regulations.

Controls by the Private Sector?

Although the Privacy Protection Study Commission recommends some areas of federal regulation, most of its proposals look to the private sector to develop and to enforce privacy constraints. There are some examples of industry leadership to develop information management principles in conformity with fair information practices but, as previously noted, the progress is slow. Informational privacy cannot be enhanced without changes in the way personal information is managed, and those changes may entail additional business costs. Especially in times of economic stress, the private sector will be reluctant to undertake new costs in behalf of a murky concept of "privacy," especially if there are no active pressures in the market place to do so. The conferees expressed doubt about the practicality of relying on the market place for privacy protection. Consider these examples:

PARTICIPANT NO. 1: The argument that simple trade association or other involvement will work may not be terribly persuasive. It's not particularly in the interest of trade associations to make a big stink about privacy questions.

PARTICIPANT NO. 2: Because of a lack of public awareness, the people who are putting information systems into the market place don't hear a public demand for privacy protection. Even though there are some standards within the industry, the risk is that the industry itself would ignore the standards and, simply because of cost, fire the computer guy who wanted to obey those standards.

Bargaining in the market place might be a way to determine privacy constraints, with customers negotiating and paying for informational privacy protection. For instance, a bank customer might agree to pay an additional monthly service charge for the assurance that certain procedures to guarantee informational privacy will be observed. But such an approach may be unfair if people with a valid interest in informational privacy are unable to afford it. On the other hand, perhaps those who have a high interest in protecting information may also have the ability to pay for it. Business and financial information may be an example of "ability to pay," but either side of that argument is mere conjecture at present.

□ □ □

Conclusion

While the conferees brought the symposium to a close with a feeling of accomplishment regarding improved understanding and insights, nevertheless they were not convinced that informational privacy would be enhanced significantly in the 1980's. From some perspectives it seems as if George Orwell's *1984* is already here, although it was also observed that the problem may not be massive invasions of privacy by "Big Brother's" giant computer, but the atrophy of privacy resulting from "Little Brother" tinkering with his personal computer next door.

The network of those who press for the development of informational privacy may enlarge both in size and activity, and perhaps a privacy constituency will emerge. The challenge remains to develop a fair information policy that respects individual integrity while accommodating the enrichment of life through an advancing but humane technology.

□ □ □

A Postcript: The Plan For Action

In light of the urgency expressed at the symposium for continuing efforts to explore and explain issues of privacy in an environment of sophisticated information technology, we were not satisfied to leave the matter of follow-up unresolved. The time constraints of the symposium did not permit further consideration of an action program at the conclusion of the meeting. Accordingly, a further consideration of the matter was undertaken following the Amelia Island conclave.

A planning committee met for two more days to consider what further action might be appropriate. Though it was considered unwise and premature to suggest a single ongoing mechanism to stimulate development of an informational privacy construct, the planning group did agree on a format for an annual dialogue series as a focus for assessment of information privacy concerns. Planning for and a search for funding of dialogues in 1983 and beyond is underway.

Appendix A

Roster of Participants

Martha W. Barnett, Esq.
Holland & Knight
Tallahassee, Florida

Robert Belair, Esq.
Kirkpatrick, Lockhart, Hill, Christopher & Phillips
Washington, D.C.

H.W. William Caming, Esq.
American Telephone & Telegraph Company
Basking Ridge, New Jersey

Prof. Gordon C. Everest
University of Minnesota
Minneapolis, Minnesota

Lewis Goldfarb, Esq.
Federal Trade Commission
Washington, D.C.
(currently with Hirschkop & Grad,
Alexandria, Virginia)

Prof. Lance J. Hoffman
The George Washington University
Washington, D.C.

Mr. Carl W. Holmes
American Telephone & Telegraph Company
Morristown, New Jersey

Hon. Charles W. Joiner
U.S. District Court
Ann Arbor, Michigan

Peter F. Langrock, Esq.
Langrock, Sperry, Stahl & Parker
Middlebury, Vermont

Hon. George N. Leighton
U.S. District Court
Chicago, Illinois

Prof. David F. Linowes
University of Illinois
Urbana, Illinois

Prof. Alfred R. Louch
Claremont Graduate School
Claremont, California

Prof. Robin W. Lovin
The University of Chicago
Chicago, Illinois

Prof. M. Granger Morgan
Carnegie-Mellon University
Pittsburgh, Pennsylvania

Dr. Elmer R. Oettinger, Jr.
Professor Emeritus
University of North Carolina
Chapel Hill, North Carolina

Mr. Donn B. Parker
SRI International
Menlo Park, California

Dr. Carolyn R. Payton
Howard University Counseling Service
Washington, D.C.

Prof. George B. Trubow
John Marshall Law School
Chicago, Illinois

Dr. Sherry Turkle
Massachusetts Institute of Technology
Cambridge, Massachusetts

Prof. Rein Turn
California State University
Northridge, California

Dr. Willis H. Ware
The Rand Corporation
Santa Monica, California

Dr. Fred W. Weingarten
Information Policy, Inc.
Washington, D.C.
(currently with Office of Technology Assessment,
U.S. Congress, Washington, D.C.)

Prof. Alan F. Westin
Columbia University
New York, New York

Prof. Daniel Wikler
University of Wisconsin
Madison, Wisconsin

Appendix B

Summaries of Invited Papers

The Development and Status of "Informational Privacy" Law and Policy in the United States

by George B. Trubow

The principal purpose of this paper is to discuss the development and status of privacy mainly as it relates to the collection, use, or disclosure of personal information. Much of the recent concern about privacy has resulted from the phenomenal growth of computer use, which has made it possible to collect, manipulate, and disseminate personal information in dimensions never before contemplated. Arthur Miller warned of "The Assault on Privacy" in 1964, and the public is increasingly aware of the vast quantities of personal information gathered and shared by federal, state and local government, as well as by the private sector. Personal information is defined as any information that can be referred to a specific individual by name, number, or other identifying characteristics. Consequently, it is not the content of information which makes it personal but rather its reference.

Relevant Common Law

A concept of privacy is not part of the English common law and was not specifically recognized in early American law. The idea of a legal "right to privacy" was presented in 1890 in a law review article by Samuel D. Warren and Louis D. Brandeis:

> Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops.'

The authors declared privacy to be ". . . a part of the more general right to the immunity of the person, the right to one's personality." They used the phrase, "the right to be let alone," to characterize the nature of privacy, which could be violated although the personal information published was true.

The common law of defamation is relevant to informational privacy because defamation involves the publication of false information that injures reputation. It was the falsity requirement that initially avoided conflict with the Constitution, because the Supreme Court said that the First Amendment protects truth, but not falsehood.

In 1964 the Supreme Court decided in *New York Times v. Sullivan* that there could be no liability for defamatory falsehoods about a *public official* unless the defendant knew that the publication was false or displayed reckless disregard as to whether the publication was false. In subsequent cases, the Supreme Court extended the "deliberate or reckless falsity" requirement to public *figures* as well as public *officials*. The court made it clear in *Sullivan* that the Constitution sometimes protects falsehoods to encourage free and open debate and comment.

In 1974 the Supreme Court decided *Gertz v. Robert Welch, Inc.* holding that because the plaintiff was neither a public figure nor a public official that he did not have to meet the "deliberate or reckless falsity" test required in *Sullivan*, but did have to prove that the defendant was at least *careless* with regard to the falsity of the publication. Although the Supreme Court has said that some falsehoods can be published without liability, it has not prescribed the limits on publishing truthful information, whether as to source, content, or utility. The survival of informational privacy depends upon the enforceable confidentiality of certain truthful information.

Privacy and Fair Information Practices

A government report in 1973 often has been cited as the first major contribution to the development of a rational policy regarding personal information: "Records, Computers and the Rights of Citizens," by the Special Advisory Committee to the Secretary of Health, Education and Welfare. The report noted the significant growth of the use of computers to process information and proposed a set of "fair information practices" whose purpose was to enhance personal privacy by protecting the confidentiality of personal information. These principles may be distilled as follows:

1. Collect only that personal information necessary for a lawful purpose.
2. Use only decision making data that is relevant, accurate, timely, and complete.
3. Give the data subject access to information about himself and a procedure by which to challenge and correct the information.
4. Use data only for the purpose for which it was collected.
5. Protect the data against unauthorized loss, alteration, or disclosure.

The Privacy Protection Study Commission, established by the Privacy Act of 1974, conducted a thorough and comprehensive study of public and private record systems and issued some 166 specific recommendations to enhance informational privacy. While acknowledging the soundness of the foregoing principles, the Commission articulated three objectives of good information practice: (1) to minimize

intrusiveness to the personal affairs of citizens, (2) to maximize fairness to individuals in the way personal information is managed, and (3) to legitimize expectations of the confidentiality of personal information.

Federal Laws

The Privacy Act of 1974 deals with personal information stored by federal agencies only and provides for access by data subjects, procedures to correct and amend challenged information, and limitations on disclosures to third parties. The other significant federal laws protect information held by some private sector entities.

The fair information practices and objectives seem reasonable on their face. It is in the application of these principles to differing information systems that difficulties arise. Record system managers disagree about how the principles of fair information practices should be interpreted.

The Fair Credit Reporting Act (FCRA) of 1970 requires the credit investigation and reporting organizations to make their records available to the data subject, to provide procedures for correcting information, and to permit disclosure only to authorized customers. The Crime Control Act of 1973 requires that state criminal justice information systems developed with federal funds insure the "privacy and security" of information. Department of Justice regulations impose some restrictions on the dissemination of criminal history record information. The Family Education Rights and Privacy Act of 1974, popularly referred to as the Buckley Amendment, requires schools and colleges to grant students (or their parents) access to student records, provide challenge and correction procedures, and sharply limit disclosure to third parties. The Right to Financial Privacy Act of 1978 provides bank customers with some privacy regarding records held by banks and related institutions. The Act provides procedures by which federal agents may gain access, but the law does not cover state or private sector third-party inquiries to banks.

Although these regulations provide some protection, there is no governmental regulation of employment and personnel, health and medical, or insurance information, and the record systems of private organizations generally are unregulated.

The Freedom of Information Act of 1966 (FOIA) makes federal records available for public inspection and copying, on the theory that the government's business is everyone's business. A specific exemption from the law's requirements is for disclosures that would be a clearly unwarranted invasion of privacy. This exemption deals with cases in which a government record may pertain to an individual other than the one making the inquiry. Balancing the public's "right to know" against an individual's desire for privacy is a tricky task, and there is no sure formula to give consistent results.

State Laws

State legislatures also have supplemented common law protection by providing some specific information confidentiality guarantees. Most states do have their own brand of FOIA, and the same conflicts with confidentiality statutes are encountered here as in the federal arena.

Criminal justice and medical and tax records receive attention by many states. Conviction records are usually not restricted, and it is common for data subjects to have rights to inspect and challenge recorded criminal history information. A majority of states provide confidentiality to medical and tax records, respecting the doctor/patient relationship and the financial privacy of the taxpayer.

Fewer than 20 states protect the confidentiality of bank records in parallel to the federal law, and a similar number have provisions to supplement FCRA protection.

About 20 states have some sort of general privacy law, either in their constitution or by statute, but on the whole such measures are narrow and relatively insignificant. Informational privacy thus far has been a popular subject for state inquiry, although there is not much legislation to show for it.

The National Conference of Commissioners of Uniform State Laws, in 1980, approved the draft of a Uniform Fair Information Practices Code. That proposal includes both FOIA and privacy provisions, each modeled largely after the federal acts. The major benefits of the draft are that it makes FOIA and privacy more compatible in implementation, it avoids some of the problems experienced at the federal level, and it provides a broad and comprehensive basis for managing information held by state and local government. The UFIPC draft does not, however, seek to regulate information in the private sector.

Conclusion

Whatever may be the bounds of privacy defined by various federal and state case precedents, statutes, or regulations, the notion does not have an intellectual foundation; what doctrine there is appears to be the result of emotion and value perception rather than that of any rational limits on disclosure of personal information based on reasonable and enforceable expectation. Even the generally accepted "principles" of fair information practice are subject to claims of exception and exclusion whenever applied to any particular information system. "Those rules are good for others but not for me . . ." is a frequent judgment rendered by an information system manager. Federal and state executives, legislatures, and courts promulgate or declare more or less privacy, but they have produced a patchwork quilt and not a fabric woven from the fiber of consistent and uniform interests.

Information Technology and Privacy Trends in Products and Services

by Fred W. Weingarten

This paper surveys the developments in information technology—products and services—as they are likely to evolve over the next decade and as they may possibly affect individual privacy. The predictions are surprise-free and are based on technology currently existing in the field or laboratory. They assume no specific legislative, regulatory, or market barriers to commercial development.

General Trends

A number of general trends in information technology affect the nature of products and services that will be available over the next decade:

1. Although small computers will become common in the home and office, products that incorporate microcomputer chips will be even more numerous.
2. Computer-based products and services will be mass produced and will be widely available at affordable prices.
3. Information products and services will be increasingly based on combinations of computer, communication, and video technology.
4. Electronic forms are growing increasingly cost-competitive with paper for storing information.
5. An information market place is growing, in which information is treated as a valuable commodity—produced or collected, packaged and sold for profit.
6. The number of very large integrated data systems will grow—systems that may be either highly centralized or composed of several small systems linked together by data communication lines.

On the assumption that the privacy impacts of information technology will be felt principally in terms of the environment in which it is used, the following discussion has been oriented around these environments.

Information Technology and the Person

Three important trends are changing the potential of information technology to collect information directly from the individual:

1. Micro-miniaturization of electronics increases the portability of information technology.
2. Improvement of sensory instruments allows for sophisticated, unobtrusive monitoring of bodily functions.
3. New telecommunications technologies will facilitate direct links with individuals, no matter where they are.

Products and services that could become available include portable information tools such as the hand-held computer or terminal and the "smart card"—a microprocessor on a credit or identification card. Also likely are medical devices for passively measuring bodily functions, transmitting the information, and even providing medication or electrical stimulus.

Information Technology and the Home

Five major trends characterize the use of information technology in the home:

1. Many, perhaps most, common consumer devices in the home will contain microprocessor chips.
2. Many homes will have desk-top computers.
3. A variety of new entertainment media and programming will be available for purchase or on a pay-for-service basis.
4. Communication lines into and out of many homes, via broadcast and wire, will have much more information carrying capacity by the end of the decade.
5. Homes will be linked to a variety of outside information systems including electronic mail, electronic banking, in-home shopping, teletext and videotext, and home security services.

In sum, the home will experience a rapid growth, both in computational and data storage capability and in the capacity of communication links that carry information in and out. Appliances already are being equipped with computer controls and memory capability. Video cassettes and video disks offer new means for storage and playback of information. Two-way cable systems, low-power television, direct broadcasting satellite, cellular radio, and upgrades to the local telephone loop will all provide data communication facilities to the home that are vastly superior to those now available.

Information Technology at Work

Information technology will have a profound impact on work—on the kinds of work we do and how we do it, where we work, the organizational structure of the work place, and the relationship between employees and employers in organizations. Specific trends are as follows:

1. Robotics and other computer-based technology will transform the U.S. manufacturing industry.
2. Word processing is only the leading edge of a wholesale automation of white collar office work that will take place during the next decade.
3. The professions, such as medicine, engineering, and law, will become increasingly dependent on the use of automated information services.
4. Employees whose jobs are principally handling information may be geographically dispersed through work at home, local office centers, or other patterns of distribution.

A number of privacy issues may be raised by work place automation. For example, an automated machine used by an employee may be continuously collecting performance data leading to increased employer surveillance of employees. In addition, more employee data of all types will be stored in electronic form, making it easy to search, to transmit, and to match with other personal data files.

Information Technology and Society

A number of broader societal products and services with which a citizen interacts will also be changed by information technology.

For example, banking will increasingly be done electronically, through such services as automated tellers, point-of-sale debits, and pay-by-phone arrangements. With such systems, more personal information will be collected and stored in computer-readable form. Financial data bases will be integrated as instructions offer a broader variety of financial services, and they will be linked into nationwide networks. Finally, payment alternatives used by individuals who wish to protect their privacy may gradually disappear.

The market place will place increasing emphasis on using computers and communication technology to target sales efforts at narrowly defined consumer groups. This trend will place a premium on collecting and selling personal data for use in marketing applications such as compiling mailing lists for direct sales, testing and monitoring consumer behavior, measuring the effectiveness of advertising campaigns, and determining audience profiles.

Government and political use of information technology will affect the individual as a citizen. Government agencies operate large data systems containing personal information on millions of individuals. These systems will continue to grow, both in size and in the amounts of information held in each. In addition, pressures for efficiency will continue encouraging government to integrate the data bases of different agencies. The practice of matching (comparing information in one government data system with that in another) will also likely increase, for purposes such as determining possible criminal behavior or identifying questionable use of social benefit programs.

Morality and Privacy

by Alfred R. Louch

We can take for granted that most of us want privacy and know what it is when we find it. But here unanimity ends. We feel the need for privacy in different ways and to different degrees, depending on the varying circumstances of our lives. And we lack a consensus as to what kinds and extent of privacy claims are justified, what sort of legitimate burdens and restrictions these claims place on other individuals and institutions to respect them. So the question is not what privacy *is*, but whether and to what extent it is a right.

The theme of this conference relieves me of the obligation to sort out the variety of contexts in which privacy is claimed as a right. We ask here the more limited question: to what extent (and why) may the individual control the collection and dissemination of information about him? This is like the question: when is a person within his rights in wanting to be observed? In that case, one might object to the mere fact of being observed, as much as to the potentially harmful consequences of personal information obtained by another. This is why we don't like spies, whether they are malicious or merely curious. Similarly, we may resent the storage of information about us because we fear it may be used to affect us adversely; but we may also object to its collection simply because it is an instance of spying, a more than casual scrutiny of what we are up to, even though what is recorded is innocent and trivial.

Our intuitions about spying may go some way toward justifying and charting acceptable limits of information storage. Data banks, although possibly casual collectors of information, are in effect overdiligent observers of individual behavior. Our objection to storage of information thus has a source other than that derived from an adversarial conception of person/person and person/state relationships. That model limits the vulnerability of individuals to one another and the state, thus guaranteeing some measure of personal autonomy. Invasions of privacy will then be seen as threats to our favored political order and to our system of law. But the indiscriminate collection of personal data threatens our conception of ourselves as persons and as moral beings.

I do not believe that invasions of privacy can be perceived as so fundamental if we suppose we confirm our moral convictions through calculations of utility. For then privacy is merely one among many values,

prized only to the degree to which one is more promising. That view makes respect for persons central and invulnerable to calculations of policy. A community in which the individual is primary can be readily pictured by seeing individuals as citadels protecting a rich interior life from public scrutiny or manipulation. If our minds become perfectly transparent to others, we would cease to be that kind of being. Data collection systems increase that transparency and so assault our personal integrity, in a most profound way. The result is that our moral universe, our conception of ourselves in relation to others, is radically transformed.

I conclude with two demurrers to this defense of informational privacy. First, our conception of private persons is nurtured within the segment of society most able to profit from the immunities flowing from that conception, those who can afford space, walls and other shields from the curious and the malicious. So privacy may be protected only at the expense of equal treatment.

Second, our highly individualistic conception of personal integrity is nurtured by an environment which communities have not always enjoyed and which our world community may be on the verge of losing. A future plagued by inadequate resources, declining productivity, and growing population may soon be unable to afford the luxury of individualism and the sense of privacy that flows from it.

A Taxonomy for Privacy

by Willis H. Ware

The invitation to present this paper suggested that it might seek to organize privacy concerns in some overall framework. The legal, judicial, and legislative communities—as influenced by moral and ethical views—are dealing with privacy issues one by one as they arise. There seems to be no cohesion presently across the fabric of privacy.

A suitable framework must accommodate technology, such privacy law as has already been created, and the moral and ethical views of society. One approach is to imagine the privacy consequences of new technologies, but it would all be speculation about things that are possible in principle but might never happen. Instead, the discussion here attempts a pragmatic look at the broad sweep of privacy and is oriented toward providing the legal and judicial communities a way of looking at privacy litigation and possibly also a way for the legislative community to think about new law.

Any discussion of technology will always point out its rapid progress and the profound effect it is likely to have on society, especially when the technology is related in some way to information or data. Such products as hand calculators, personal computers, various cable services, wired cities, and on-line data bases can—in some scenarios—create privacy consequences in principle, but they do not automatically give rise to privacy difficulties in fact and may never do so, depending on details of the utilization. Since the world has made an irrevocable commitment to computer technology, the days in which affairs could be conducted by paper and pencil under green eyeshades are forever gone. Society must deal with the consequences, one of which is information.

Philosophically, awkward moral and ethical issues arise when one seeks to define privacy, in part because the very word "privacy" connotes such diverse concepts to individuals. We do not really know what privacy is in a comprehensive way, but individuals certainly believe they know it when they see it. What is needed is a framework for recognizing a privacy infraction and deciding what to do about it when it occurs. Rather than trying to define "privacy," define instead "invasion of privacy" and develop an overall construct from that point of view.

Consider the notion of "space" in the context of personal surrounding. To illustrate, visual space is what is accessible to eyes; aural space, what ears catch; physical space is a cocoon of certain dimensions around a person. More abstract is the notion of informational or record keeping space, but one's imagination can see a volume that includes all the records that concern one's life.

If we envision a "space" as a physical volume, then we can also envision an intrusion or entry into such a space. Negative or undesirable consequences of an intrusion can be catalogued and separated into annoyances: those that constitute harm and those that should be overlooked or ignored. The harmful ones will constitute the definition of what "injury" means for the space in question; we can then decide what legislative actions or judicial insights are needed to deal with each space and its intrusions.

Try some examples. Visual space is what the eyes see. Intrusions include flashing bright lights, the display of objectionable materials, or critical written attacks. Consequences of such intrusions include annoyance, anger, or damage to reputation. Some of these consequences might be legally actionable under existing law dealing with obscenity or defamation.

Aural space is what is heard by the ears. Typical intrusions would include loud music, casual conversation, excessive noise, shouted remarks or obscenities. The consequences of intrusion could include annoyance, physical damage, pain, or anger. Some of them might be legally actionable; others would not.

Intrusions into one's physical space would include standing close, sitting on the same bench, physical

pressure in a crowd, touching and fondling, or bodily confinement. The consequences could include annoyance, discomfort, psychological malice, sexual affront or bodily harm. Some of these might be actionable under the laws of assault, battery, or false imprisonment.

With respect to record keeping space, intrusions might include misuse of information, improper dissemination of information, or collection of inappropriate facts. Consequences could include embarrassment, denial of credit, or destruction of reputation. The privacy invasion of record keeping space is legally actionable to some extent under various federal and state laws.

In defining invasion of privacy rather than privacy itself, the steps are these: identify a space of concern; identify possible intrusions; identify the consequences of each intrusion (here moral and ethical views of society are involved); determine what "injury" is for each intrusion (again, consider the moral and ethical views of society); and, finally, address the question of legal actionability. Clearly the overall judicial process and legislative attention would be folded in.

The validity of such a "backend-to" procedure is encapsulated in the following series of points:

- It concentrates on events and relates them to societal views, morals, and ethics as exemplified through the legislative and judicial processes.
- It tracks and reflects usage of technology rather than *a priori* proscribing acceptable boundaries for it.
- It accepts any legal actions that are appropriate to the hurt, *e.g.*, recover damages, penalize, or enjoin the perpetrator.
- It accommodates expressions of concern by society in behalf of individuals, individuals in behalf of themselves, or society in behalf of its institutions and organizations.

The proposed construct—or taxonomy for privacy—might be used as an analytic framework for perceiving the privacy consequences of some new use of technology, or for identifying areas where legislative attention is needed. For this purpose, one would decide what space some new service might intrude, imagine the intrusions and consequent hurts, and design safeguards or laws to protect against them. Perhaps the notion of space—which is a concept borrowed from the physical sciences—together with an easily grasped idea of intrusions into a space, can usefully add scope and fullness to an insightful idea expressed many decades ago.